#21/L

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant and Inventor	Ho Keung, TSE.
Filing Date	07/09/98
Application Number	09/112,276
Group Art Unit	2132
Examiner	Gilberto Barron Jr.
Postal Address	P.O. Box 70492, KLN Central Post Office, Hong Kong.
H.K. Tel & FAX	(852) 8105, 1090 (852) 8105, 1091
Email	t9224@netscape.net

By Airmail & Fax

Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Sir,

Amendment dated March 10 , 2002

The Examiner is respectfully requested to enter this amendment, otherwise even if the present application is patented, a reissue patent application for broadening the scope thereof will be inevitable.

I have just happened to find that the office can now accept a software patent to claim a program stored in a media. This is contrary to the instruction of Examiner Mr. Pinchus M. Laufer of the mother application that "a program must be used in a computer". Although the Examiner of the present application does not raise such a rejection, unfortunately I have been following closely to this instruction of Mr. Laufer when amending the claims, with a view to avert unnccessary rejections, this make the scope unreasonable and can easily be circumvented.

I hope the Examiner can understand.

Submitted herewith is also a remark filed with a view to preclude any possible rejection basing on US Patent 5,586,186, issued to Yuval, et al, published on Dec 17, 1996 .

Also submitted herewith is a table indicating the # of times of amendment of each claim for each amendment letter filed. From this table, the Examiner will find that the # of times of amendment indicated in some "dirty claims" is incorrect. For instance, the # of time of claim 12 being amended in Amendment Proposal Dated 22 June 2001 is incorrectly indicated in the dirty claim 12 therein as "Three Time Amended", and actually it is "Four Time Amended". To indicate this errors in the table, the "<u>4</u>" is **underlined.**

New claim 22 submitted. 22 claims presented, in which claims 1, 7, 10, 12, 14, 16, 18, 20-22 are independent. Claims 1-3, 7-12, 14, 16, 18, 20 are amended.

Note that claim 3 depends on independent claim 12, not 1.

Note also that claims 1, 10, 12, 14, 18, 20 as amended herein are further amendment of claims as submitted in "Amendment dated 25 Jan., 2002".

Replacement sheets 13, 15- 19, 21 and new sheet 23 are submitted therefor.

Claims 9, 11 as amended now recites "<u>computer readable medium being data signal embodied in a carrier wave</u>" **is not new matter**. Note that the "authorising software/program" existing in the medium as readable on claims 7, 10 respectively upon which claim 9, 11 depends respectively, corresponding to "the A/S sub-program in the central program" of the description and as readable on sheet 7, last paragraph, lines 1,2, "the central program is being installed in a harddisk of a user computer", this implicitly indicates the central program which may be obtained from a disk or internet, is being transferred to the harddisk in the form of data signal embodied in a carrier wave.

Claim 20 recites "the presence of identity information/means in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform … step (a). This actually means that the protection software determines the presence of identity information/means, like claim 1, or combined with the identity information/means in a non-separable manner, like claim 7.

Respectfully submitted,
Ho Keung, Tse.

Comment on Yuval et al.

This comment is filed with a view to preclude any possible rejection basing on US Patent 5,586,186, issued to Yuval, et al. This is one of the endeavours I made, as an applicant, without any deceptive intention for ensuring the present application if will be granted, will be a valid patent throughout its term.

Yuval, et al should be a closer reference compared with any reference in the search report.

The Examiner is respectfully to consider it, as make formal indication as to his acceptance to the comment.

As Yuval et al. was published on Dec 17, 1996, after the priority date Dec 1, 1995 of the present application, therefore **any rejection so raised should be 35 U.S.C. 102(e).**

As readable on claim 1, the patent is directed to a method for controlling unauthorised access to information distributed to users, comprising the steps of:

......;

encrypting the information;

receiving identifying information(ID) from a user;

generating a numeric representation(X) of the ID ;

generating a unique user key(Y) using X and decryption key of the encrypted information ;

providing the user with the unique user key ; and decrypting the encrypted information using X, Y.

Other claims such as claim 21 recites 2 numeric representations and 2 unique user keys etc, but principle behind them and claim 1 are the same.

And, as readable on col. 7 last paragraph-col. 8 first paragraph, ID can be determinable from XY & X, so as to trace the user who reveals them to an unauthorised user.

Further, Yuval et al also suggest, "To provide a higher level of security, the identifying information should include information that the user would not want to divulge to others (e.g., a credit card number…)".

Thus, Yuval et al's patented invention is similar with the present application in that it discloses protecting software, by requiring the present of user identity information as a precondition for accessing software .

Yuval et al's patented invention has the following drawbacks :

1) **No "Psychological Barrier Effect"** as taught by the Present Application

Although not explicitly indicated in Yuval et al's document, once a user enters his ID and user key Y into a computer, they will automatically converted into information in a machine-readable only form storing at a location unknown to any user.

In other words, even if the ID including credit card information, it is **not capable of being used in enabling electronic commerce operation(s)** and this is required by my independent claims 1,7, 10, 12, 14, 20.

Further, it would not be possibly expected that it could provide the "psychological barrier effect" as suggested by the present application. Unless an inventive step is being made for converting the machine-readable only form information storing at the unknown location into to a user accessible form, such as causing a display thereof.

And, without expecting the "psychological barrier effect", it would further impossible for one with ordinary skill in the art to **permanently** storing the machine readable only form information in that unknown location, rather than the decryption key or the product XY obtained there from, for eliminating the hassle of repeatedly entry of ID and user key by user. As the latters can be used more directly for decrypting the encrypted information, and as mentioned above, Yuval et al disclose that XY can also be used to trace the user.

Accordingly, Yuval et al's patented invention cannot meet claim 7 as claim 7 requires "identity software used on said processing apparatus in enabling <u>electronic commerce</u> operation(s)", it also cannot meet claim 10 as claim 10 requires "information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible".

Finally, even if it would be obvious to one with ordinary skill in the art to use <u>e-wallet</u> as Yuval et al's ID, it would not be possible for one to combine the e-wallet with a program comprising Yuval et al's method in such a manner that **the program is prevented from being copied there from individually**, and therefore cannot meet claim 7. Further, e-wallet also cannot meet claim 10 as claim 10 requires the "information capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, ..**not being** **~~usable~~** executable 'directly by said processing apparatus for said electronic commerce purpose".

2) No Machine Authentication/Determination of Existence of ID

It should be noted that Yuval et al's patented invention will use any user ID, even if it may be incorrect, to generate a "decryption key" which may also incorrect. Further, it will use the key so obtained to "decrypt" the encrypted information and the "decrypted information" may actually "random numbers" and cannot perform as the original information should be.

So, it is up to a human to determine whether the ID inputted is authentic. When a human note that a computer is performing improperly or even when the software/hardware thereof being damaged, he may then know his computer should be actually executing a series of random numbers, rather than a correctly decrypted program, if he is smart enough.

A software vendor has no right to cause an unpredictable damage to a uscr's computer, evcn if he is using pirate software. Further, this may be caused by just somc minor errors in ID entry by a rightful user.

This "random numbers" problem would not be obvious to one with ordinary skill in the art, and therefore, one would not be capable of overcoming it. Even worse, this problem is inherent in Yuval et al's patented invention and is impossible to eliminate unless using another approach completely different .

The present claims 1, 12, 14 requiring authentication/determination of existence of identity information and using a favourable result thereof as a pre-condition for providing access to software protected preclude this problem automatically.

# of times of Claims Amended

Claim number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Formal Amendment Dated April, 02, 2001	2	1	1	1	1	1	2	1	1	2	1	2	1	2	1	1	New claim 17-20 Submitted.				
Amendment Proposal Dated 7, May 2001			2													2	1	1	1	1	
Amendment Proposal Dated 17, June 2001	3						3			3		3		3		3				2	
Amendment Proposal Dated 22, June 2001	4		3			2	4			4		4		4		4		2	2	3	
Submission of Clean Claims dated 25 June 2001	Amend claims 7, 19 to clear minor typographical errors																				
Submission of New Claim 21 & Amendment on Description	Submit new claim **21**, amend minor error in claim 19, amend description and the title being last time amended to be read as "Computer Apparatus/Software Access Right Management"																				
Amendment on Claim 18 Dated Oct., 17, 2001																		3			
Amendment on New Claim 21 Dated Oct., 19, 2001																					1
Last Amendment Dated Oct., 20, 2001																					2
Informal Communication to Examiner Barron Date: Nov., 5, 2001																		4		4	3
Amendment dated 25 Jan., 2002	5									5		5		5				5		5	
Amendment dated March 10, 2002	6	2	4				5	2	2	6	2	6		6		5		6		6	

Independent Claims : 1,7, 10, 12, 14, 16, 18, 20, 21

1. A method for protecting software from unauthorised use, comprising the steps of:

determining if identity means/information, is existing in a processing apparatus ;

using a favourable result of said determination as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein :

said identity means/information, if so existing, being capable of being used in enabling electronic commerce opcration(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s).

2. A method for protecting software from unauthorised use , as claimed in claim 1, whcrein further comprising thc stcps of :

authenticating said identity means/information ;

determining said identity means/information as existing, if the result of said authentication is favourable and as not existing if otherwise .

3. A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected bcing first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;

wherein further comprising second software for, when bcing executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and for providing uscr access to third software if said authentication result is favourable .

7. A computer software product for protecting software publicly distributed against unauthorised use ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected ;

wherein :

said identity program code and said authorising software are contained in said software product in such a manner that said authorising software is prevented from being copied therefrom individually; and

the improvement resides in said protection basing on no hardware and/or software specific to said rightful user(s) other than said identity program code and said identity program code being specific to said rightful user(s) ;

and said identity program code and said authorising software existing in a computer readable medium .

12

u'

8. A computer software product as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful user(s) .

9. A computer software product as claimed in claim 7, wherein said authorising software contains said identity program code and said computer readable medium being data signal embodied in a carrier wave.

-16(Clean Claim)-

10. A computer software product for protecting other software against unauthorised use, comprising :

authorising program for providing user access to said software desired to be protected;

wherein :

information specific to rightful user(s) of said software desired to be protected, exists in said authorising program as a part thereof and being accessible to the user thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being executable directly by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said processing apparatus as a part thereof;

said authorising program existing in a computer readable medium .

L2
con't
Sell
H'
U'

11. A computer software product as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s) and said computer readable medium being data signal embodied in a carrier wave.

12. A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed.

13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

14. A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with a processing apparatus;

using a favourable result of said authentication as a pre-condition for causing said processing apparatus to provide uscr access to said softwarc desired to be protected ;

wherein said identity information/means existing in such a manner that said identity information/means being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s).

15. A method for protecting software from unauthoriscd usc , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

-18(Clean Claim)-

~~16. A method for protecting software from unauthorised use , comprising the steps of :~~

~~(a) obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;~~

~~(b) determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with second information therein ; thereafter~~

~~(c) authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;~~

~~(d) using a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;~~

~~wherein said second information being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible ; and said method is being performed without causing a said transaction take place .~~

L2/
mh 4

Sub K2

U1

~~17. A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.~~

12/ con't
U'

18. A method for protecting software from unauthorised use, by restricting the use thereof to a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being obtained from said processing apparatus ;

(c) using a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

(d) authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

(e) using a favourable result of said authentication as a pre-condition for permitting use of said software on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thercafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

20. A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use ; comprising a sub-method ;

~~13~~ 21

wherein said sub-method a protection software being used and "the presence of identity information/means in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information/means being specific to said user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a) determining by said protection software running on a processing apparatus, say, first processing apparatus with said precondition being met, first infonnation related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining if said second information is consistent with said first information ;

(d) using a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to bc protcctcd on said sccond processing apparatus ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

Rule 126
6Q 8/1/02

22
(NEW Claim)-

22. ~~23~~. A softwarc product comprising computer code for causing one or more processing apparatus to perform the method of claim 1, 12, 14, 16, 18, or 20;

said ~~compt~~ computer code existing in a computer readable medium.

Sub M3

1.(Sixth Time Amended) A method for protecting software from unauthorised use, comprising thc steps of:

determining if identity means/information, is existing in a processing apparatus ;

using a favourable result of said determination as a prc-condition for causing said processing apparatus [providing] to providc user access to said software desired to be protected ;

wherein :

said identity means/information, if so existing, being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

[wherein] access to said software desired to be protected is being provided without causing a said operation being performcd and said identity means/information being specific to said rightful user(s) and said software desircd to bc protected being licensed to said rightful user(s).

2. (Second Time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/information ;

determining said identity means/information [will be determined] as existing, if the result of said authentication is favourable and as not existing if otherwise .

3. (Fourth Time Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardwarc and/or software of said processing apparatus ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and for providing user access to third software [will be provided] if said authentication result is favourable .

-15(Dirty Claim)-

7. (Fifth time Amended) [Protection] A computer software product for [use on a processing apparatus, to protect] protecting software publicly distributed against unauthorised use ;

said [protection] software product comprising :

identity program code for [software used on said processing apparatus, in] enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected ;

wherein :

said identity [software] program code and said authorising software are contained in said [protection] software product in such a manner that said authorising software is prevented from being copied therefrom individually; and

[wherein] the improvement resides in said protection basing on no hardware and/or software specific to said rightful user(s) other than said identity [software] program code and said identity [software] program code being specific to said rightful user(s) ;

and said identity program code and said authorising software existing in a computer readable medium .

8. (Second Time Amended) [Protection] A computer software product as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful user(s) .

9. (Second Time Amended) [Protection] A computer software product as claimed in claim 7, wherein said authorising software contains said identity [software] program code and said computer readable medium being data signal embodied in a carrier wave.

10. (Sixth Time Amended) [Authorising program/means used in a processing apparatus, to protect] A computer software product for protecting other software against unauthorised use , comprising :

[said] authorising program [/means being] for providing user access to said software desired to be protected ;

wherein :

information specific to rightful user(s) of said software desired to be protected, exists in said authorising program [/means] as a part thereof and being accessible to the user thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being [usable] executable directly by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said processing apparatus as a part thereof ;

said authorising program existing in a computer readable medium .

11. (Second Time Amended) [Authorising program/means] A computer software product as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s) and said computer readable medium being data signal embodied in a carrier wave.

12. (Fifth time Amended) A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for causing said processing apparatus [providing] to provide user access to said software desired to be protected;

wherein: said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsiblc ;

[wherein] access to said software desired to be protected is being provided without causing a said operation being performed.

13. A method for protecting software from unauthorised use, as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

14.(Sixth Time Amended) A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with a processing apparatus;

using a favourable result of said authentication as a pre-condition for causing said processing apparatus [providing] to provide user access to said software desired to be protected ;

wherein said identity information/means existing in such a manner that said identity information/means being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) and said software desired to be protected being licensed to said rightful user(s).

15. A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

16. (Fifth Time Amended) A method for protecting software from unauthorised use , comprising the steps of :

[a) creating first software with confidential information of a rightful user of said software desired to be protected therein ;

b) running said first software on a processing apparatus;]

(a) obtaining by [said first] protection software running on [said] a processing apparatus, say, first processing apparatus, first information from the user thereof ;

(b) determining by said [first] protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with [said confidential] second information therein ; thereafter

(c) [thereafter,] authenticating [by second software, the] a processing apparatus, say, second processing apparatus [onwhich said second software is being used,] basing on at least a part of said second information ;

(d) using [, by said second software,] a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on [the] said second processing apparatus [onwhich said second software is being used] ;

wherein said second information being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible ; and said [steps c) to f)] method is being performed without causing a said transaction take place .

17. A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

18. (Sixth time Amended) A method for protecting software from unauthorised use, by restricting the use thereof to a single person, comprising a sub-method ; said sub-method comprising the steps of :

[a) supplying said software desired to be protected, first software and second software to a processing apparatus, say, first processing apparatus ;

b) running said first software on said processing apparatus ;]

(a) establishing a communication between [said first software running on said] a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being obtained from said processing apparatus ;

(c) using [by said first software,] a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

[wherein a cost is being charged from said account for the first time said steps a) to e) being carried out ; thereafter]

(d) authenticating [by said second software, the] a processing apparatus [onwhich said second software is being used,] say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

(e) using [by said second sofiware,] a favourable result of said authentication as a pre-condition for permitting usc of said software [desired to be protected] on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus [if the result of said authentication is not favourable, repeat at least said steps c) to e) with said second processing apparatus] , without re-charging from said account said cost .

-21(Dirty Claim)-

20. (Sixth time Amended) A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use ; comprising a sub-method ; [the stcps of :]

[a) creating first software;]

wherein said sub-method a protection softwarc being used and "the presencc of identity information/means in a processing apparatus" is being used in the creation of said [first] protection software as a pre-condition for said [first] protection software to perform in said processing apparatus step (a) below ; and said identity information/means being specific to said user [of said software desired to be protected] and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

[b) running said first software on said processing apparatus ;]

(a) determining by said [first] protection software running on a processing apparatus, say, first [said] processing apparatus [meeting] with said precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

(b) [thereafter,] determining [by second software,] from [the] a processing apparatus [onwhich said second software is being used,] say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining [by said second software,] if said second information is consistent with said first information ;

(d) using [by said second software,] a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on [the] said second processing apparatus [onwhich said second software is being used] ;

[repeat at least said step c) with the processing apparatus on which said second software is being used if said result of said determination of consistence is not favourable] thereaftcr, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing **any** user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .